Peer-to-Peer Systems and Security

Attacks!

Christian Grothoff

Technische Universität München

June 4, 2013

"You look at this and you say this is insane. It's insane. And if it is only Hollywood that has to deal with this, OK, that's fine. Let them be insane. The problem is their insane rules are now being applied to the whole world. This insanity of control is expanding as everything you do touches copyrights" –Lawrence Lessig

GNUnet, a Framework for Secure P2P Networking

GNUnet is more than anonymous file-sharing:

- Anonymity needs company!
- Blocking an application that has many uses increases collateral damage
- Code re-use results in higher-quality code
- Anonymous file-sharing is hardly the only interesting problem

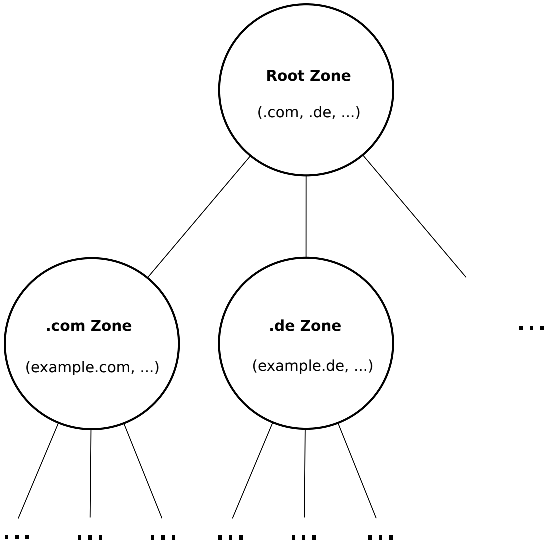
GNUnet, a Framework for Secure P2P Networking

GNUnet is more than anonymous file-sharing:

- Anonymity needs company!
- Blocking an application that has many uses increases collateral damage
- Code re-use results in higher-quality code
- Anonymous file-sharing is hardly the only interesting problem

Today: visions for GNUnet

Background: Domain Name System



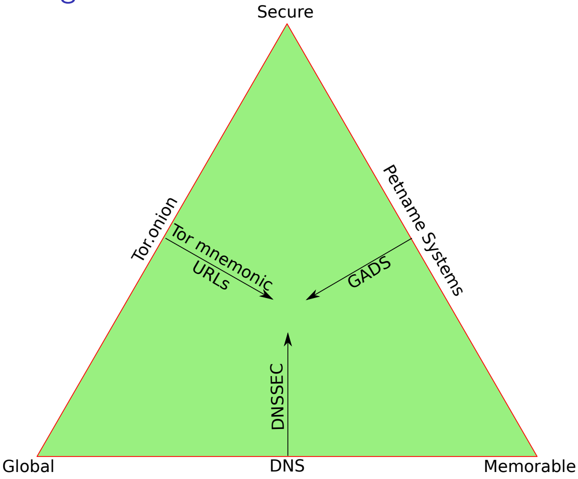
Background: Domain Name System

Wo controls the root zone? ICANN? IANA?

"The Internet Corporation for Assigned Names and Numbers (ICANN) currently performs the IANA functions, on behalf of the United States Government, through a contract with NTIA." - `http://www.ntia.doc.gov`

Secure, Memorable, Global: Choose Two

Zooko's Triangle

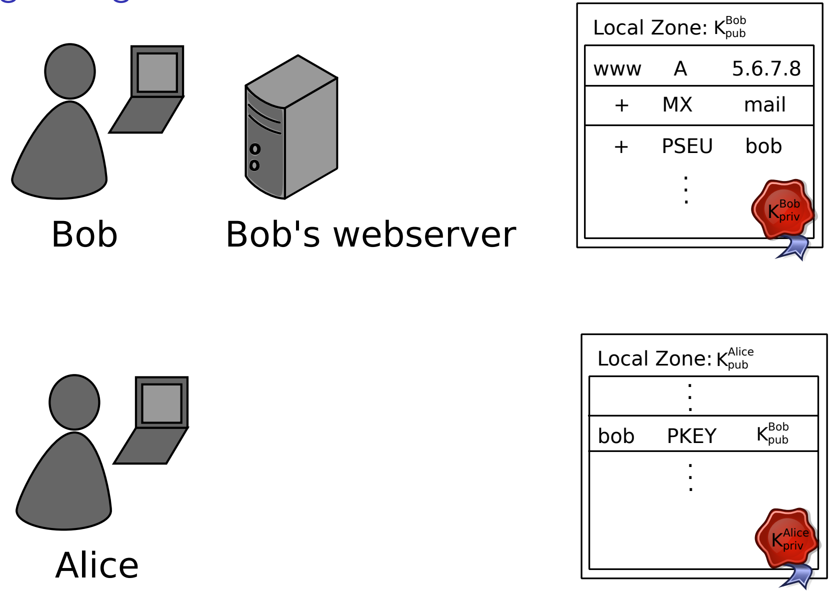


Overview

Properties of GADS

- Decentralized, distributed name system
- Secure, memorable, per-user name space in `.gads`
- Secure, globally unique name space in `.zkey`
- Linked per-user zones: *delegation*

Registering a name in GADS



Bob

Bob's webserver

Local Zone: K_{pub}^{Bob}

www	A	5.6.7.8
+	MX	mail
+	PSEU	bob
	⋮	

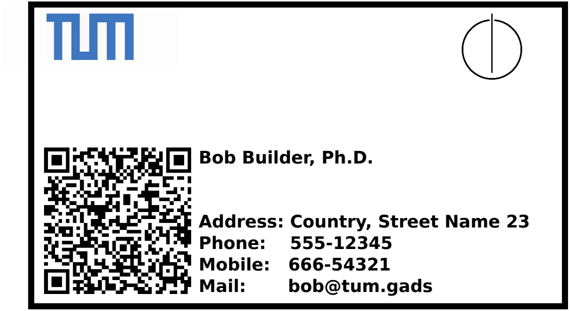
Alice

Local Zone: K_{pub}^{Alice}

	⋮	
bob	PKEY	K_{pub}^{Bob}
	⋮	

Registering a name in GADS

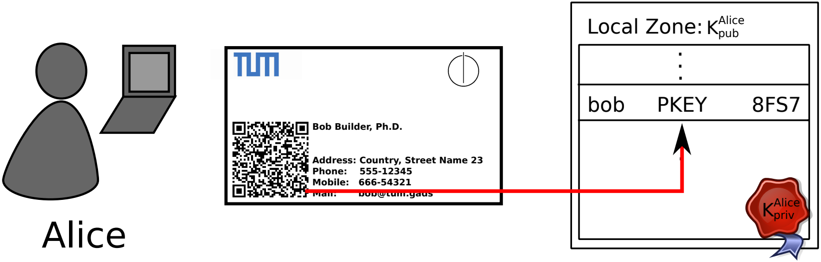
- Bob publishes his mappings in the DHT
- ... along with signatures
- Bob gives his PKEY to his **friends** via QR code:



Bob Builder, Ph.D.

Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@tum.gads

Registering a name in GADS (cont.)



Bob Builder, Ph.D.

Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@tum.gads

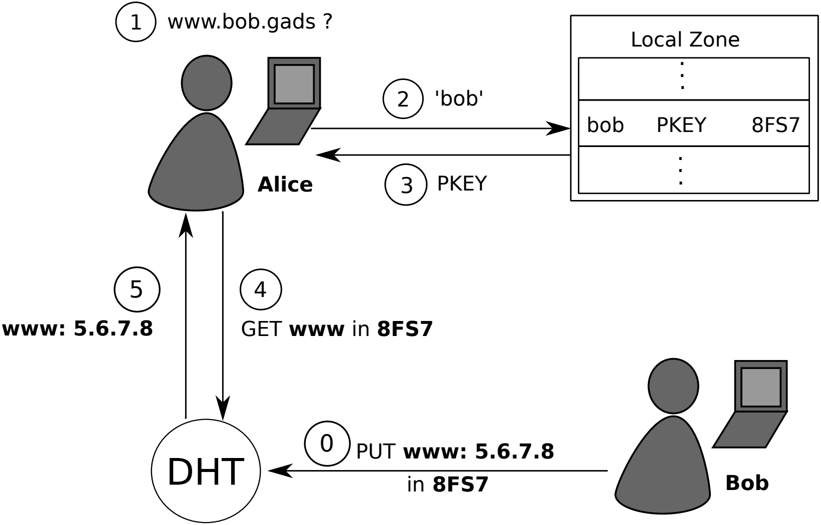
Local Zone: K_{pub}^{Alice}

⋮

bob PKEY 8FS7

- Alice learns Bob's PKEY
- Alice delegates the subdomain **bob** to Bob's zone **8FS7**
- Alice refers to Bob's webserver via `www.bob.gads` or `www.8FS7.zkey`
- How does she get the IP?

Name Resolution in GADS



From DNS to GADS

Names that are not globally unique are trouble!

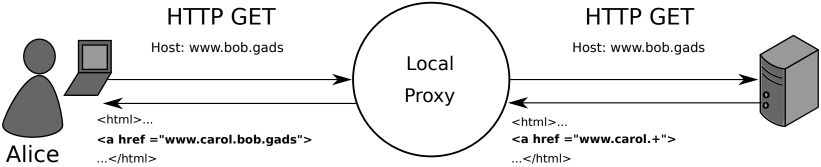
- How do we create links?
- How can we make virtual hosting work?
- How will we validate X.509 Certificates?

Solution: Relative Names

Relative Names

- Bob wants to share the link `www.carol.`**+**
- Bob interprets this name as `www.carol.`**gads**
- Alice interprets this name as `www.carol.`**bob.gads**
- Client translates names appropriately:

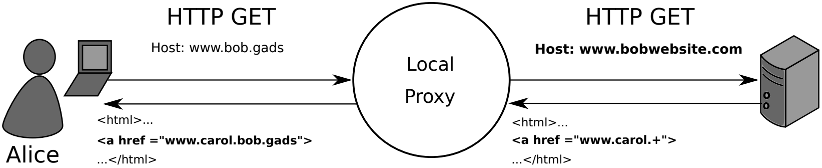
Client-Side Local Proxy



Legacy Hostname (LEHO) Records

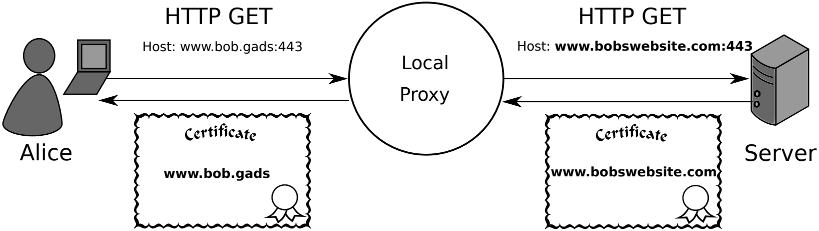
Virtual Hosting with **LE**gacy **HO**stnames

- LEHO records provide LEgacy HOstnames for names
- Example: `www(.+)` → `www.bobswebsite.com`


HTTP GET
Host: www.bob.gads
Local
Proxy
HTTP GET
Host: www.bobwebsite.com
Alice
<html>...
<a href ="www.carol.bob.gads">
...</html>
<html>...
<a href ="www.carol.+">
...</html>

SSL Certificates

Server offers certificate to client



Verification:

- Old way: Follow CA chain to “trust” anchor(s)
- Secure way: Use DANE[1] TLSA RRs!

[1] `rfc6698`

Status of Implementation and Migration

Implementation

- GADS resolver on top of GNUnet
- Client Proxy
- Zone management tools with QR export and import
- Internationalized Names (IDN)

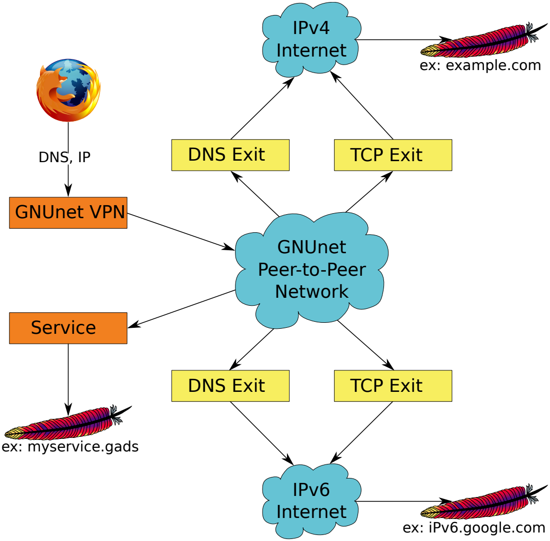
Migration

- DNS and GADS can co-exist
- DNS-to-GADS gateways
- OS integration

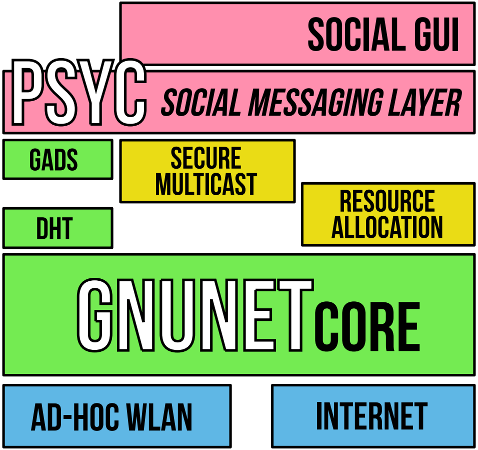
Future Work

- Reverse proxy to rewrite URIs
- TLSA verification in proxy

IPv6 Transition



Social Networking



Reuters

Democracy depends on independent reporting

- Commercialization of US news reporting destroyed US system

Reuters

Democracy depends on independent reporting

- Commercialization of US news reporting destroyed US system
- Political influence in Europe limits utility of public broadcasting

Reuters

Democracy depends on independent reporting

- Commercialization of US news reporting destroyed US system
- Political influence in Europe limits utility of public broadcasting
- Independent news papers struggle to finance investigative journalism

Reuters

Democracy depends on independent reporting

- Commercialization of US news reporting destroyed US system
- Political influence in Europe limits utility of public broadcasting
- Independent news papers struggle to finance investigative journalism
- Information overload (advertising, fast-paced global change)

Reuters

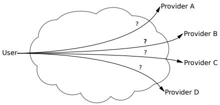
Democracy depends on independent reporting

- Commercialization of US news reporting destroyed US system
- Political influence in Europe limits utility of public broadcasting
- Independent news papers struggle to finance investigative journalism
- Information overload (advertising, fast-paced global change)
- Need crowd-sourced, crowd-edited, crowe-filtered, crowd-controlled news agency

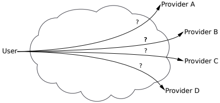
Reuters

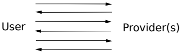
- Copy-on-write editing + references + comments (?)
- Categorization w. tags + language + timestamp
- Personalized ranking + SMC-based cooperative ranking
- Pushing via combined PoW + reputation system
- Randomization against living in personalized bubble
- TeX(t)-based

Business Platform

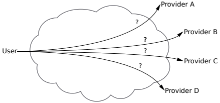


Business Platform





Business Platform



User

?

?

?

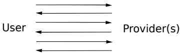
?

Provider A

Provider B

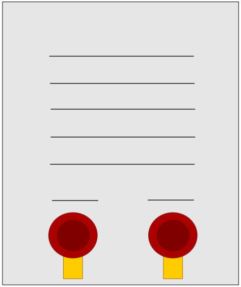
Provider C

Provider D

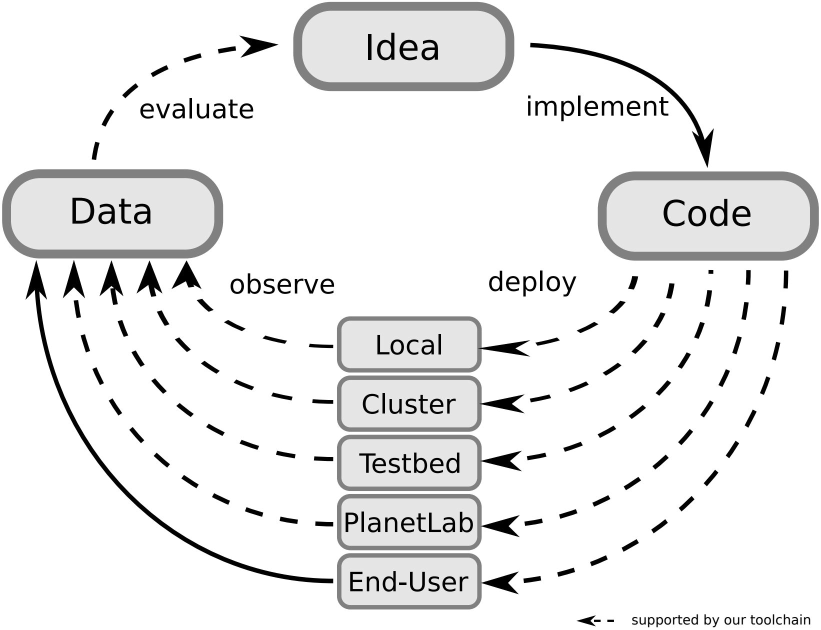


User

Provider(s)



Evaluation


Idea
implement
Code
deploy
Local
Cluster
Testbed
PlanetLab
End-User
observe
Data
evaluate
supported by our toolchain

The Free Secure Network Systems Group

Research Areas:

- Network Protocol Analysis, Design & Implementation
- Measurements & Large-Scale Experiments
- Privacy, Secure Multiparty Computation
- Constraint Solving, Optimization

Teaching Areas:

- P2P Networks
- Network Security
- DNS, IPv4, IPv6